



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/728,396	12/05/2003	Anthony J. Yeates	M61.12-0576	9252

27366 7590 04/05/2007

WESTMAN CHAMPLIN (MICROSOFT CORPORATION)  
SUITE 1400  
900 SECOND AVENUE SOUTH  
MINNEAPOLIS, MN 55402-3319

EXAMINER

HA, LEYNNA A

ART UNIT

PAPER NUMBER

2135

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	04/05/2007	PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

**Office Action Summary**

Application No.

10/728,396

Applicant(s)

YEATES ET AL.

Examiner

LEYNNA T. HA

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 05 December 2003.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-23 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-23 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 12/5/03 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

*Chankya B. Dm*  
*AU2135*

**Attachment(s)**

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
- Paper No(s)/Mail Date 3/19/2004.

- 4) ☐ Interview Summary (PTO-413)
- Paper No(s)/Mail Date. \_\_\_\_\_.
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: \_\_\_\_\_.

### DETAILED ACTION

1. Claims 1-23 is pending.

### ***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. **Claims 1-23 are rejected under 35 U.S.C. 102(b) as being anticipated by Sutter (US 6,446,092).**

#### **Claim 1**

Sutter discloses a computer-implemented method for providing data security, the method comprising:

receiving a password from a user; **(col.14, lines 47-48; a password can broadly be given in light as any form of specific information to the user such as a password, pass phrase, and PIN. Sutter refers to the claimed password as a password or a pass-phrase.)**

utilizing the password as a basis for generation of a user-specific version of an encryption component; and **(col.88, lines 58-59; the**

Art Unit: 2135

**claimed encryption component is broad whereby specification indicates components of a computer may include, but are not limited to, a processing unit, a system memory, and a system bus. Thus, with the specification reciting the component is not limited to the particular recited components, a component can also interpret as device, software application, program, or a routine. Sutter discloses the DRE cannot unlock any application database (if encrypted, the registry database), and relies on a site operator pass-phrase for each application where the pass-phrase may be varied for sites. Thus, Sutter teaches the encryption component is user specific because based on user's pass-phrase. Sutter discloses a table to show validating a password and the registry encryption key must be derived from the password using a different digest algorithm than that used to create a hash (col.48, line 60 – col.49, line 65). Sutter discloses the user password is specific to an encryption key of the application, which reads on the claimed user-specific version of an encryption component.)**

storing the user-specific version of the encryption component.  
**(col.13, lines 18-20 and col.45, lines 49-52; Sutter discloses the security and rules for each application is stored in a database and key tables)**

**Claim 2: See Sutter on col.48, line 60 – col.49, line 65; discussing a method of claim 1, further comprising: selectively allowing the user to**

Art Unit: 2135

process the user-specific version of the encryption component so as to derive the encryption component; and utilizing the encryption component to process sensitive data.

**Claim 3: See Sutter on col.89, lines 30-38;** discussing a method of claim 1, wherein storing comprises storing the user-specific version of the encryption component within a record that is associated with the user.

**Claim 4: See Sutter on col.48, line 60 – col.49, line 65;** discussing a method of claim 1, further comprising: generating an encrypted version of the password; and storing the encrypted version of the password.

**Claim 5: See Sutter on col.88, lines 58-59;** discussing a method of claim 4, wherein storing the encrypted version of the password comprises storing the encrypted version of the password within a record that is associated with the user.

**Claim 6: See Sutter on col.48, line 60 – col.49, line 65;** discussing a method of claim 4, wherein generating an encrypted version of the password comprises encrypting the password based on a one-way hash function.

**Claim 7: See Sutter on col.89, lines 43-57;** discussing a method of claim 1, further comprising: receiving a second password from a different user; and utilizing the second password as a basis for generation of a second user-specific version of the encryption component; and storing the second user-specific version of the encryption component.

**Claim 8: See Sutter on col.89, lines 43-57;** discussing a method of claim 7, wherein storing comprises storing the second user-specific version of the encryption key within a record that is associated with the different user.

**Claim 9: See Sutter on col.89, lines 43-57;** discussing a method of claim 7, further comprising: generating an encrypted version of the second password; and storing the encrypted version of the second password within a record that is associated with the second user.

**Claim 10: See Sutter on col.45, lines 50-52 and col.89, lines 43-57;** discussing a method of claim 1, further comprising: receiving an administrator password from an administrator; and utilizing the administrator password as a basis for generation of an administrator-specific version of the encryption component; and storing the administrator-specific version of the encryption component.

**Claim 11: See Sutter on col.35, lines 62-67;** discussing a method of claim 10, wherein storing comprises storing the administrator-specific version of the encryption key within a record that is associated with the administrator.

**Claim 12: See Sutter on col.35, lines 62-67 and col.45, lines 50-52;** discussing a method of claim 10, further comprising: generating an encrypted version of the administrator password; and storing the encrypted version of the administrator password within a record that is associated with the administrator.

Art Unit: 2135

**Claim 13: See Sutter on col.35, lines 62-67 and col.45, lines 50-52;**

discussing a method of claim 1, wherein utilizing the password as a basis for generation of a user-specific version of an encryption component comprises utilizing the password as a basis for generation of a user-specific version of an application security key.

**Claim 14**

Sutter discloses a computer-readable medium having instructions embedded thereon that, when executed, cause a computer to carry out a method comprising the steps of:

obtaining an encryption component; and **(col.14, lines 57-60)**  
creating and storing a plurality of user-specific versions of the encryption component; **(col.88, lines 40-59; the claimed encryption component is broad whereby specification indicates components of a computer may include, but are not limited to, a processing unit, a system memory, and a system bus. Thus, with the specification reciting the component is not limited to the particular recited components, a component can also interpret as device, software application, program, or a routine. Sutter discloses the DRE cannot unlock any application database (if encrypted, the registry database), and relies on a site operator pass-phrase for each application where the pass-phrase may be varied for sites. Thus, Sutter teaches the encryption component is user specific because**

**based on user's pass-phrase. Sutter discloses a table to show validating a password and the registry encryption key must be derived from the password using a different digest algorithm than that used to create a hash (col.48, line 60 – col.49, line 65). Sutter discloses the user password is specific to an encryption key of the application, which reads on the claimed user-specific version of an encryption component.)**

selectively allowing users to process their version of the encryption component so as to derive the encryption component; and **(col.63, lines 44-47)**

utilizing the encryption component to process sensitive data.  
**(col.90, lines 23-27)**

**Claim 15: See Sutter on col.85, lines 25-36 and col.88, lines 58-59;** discussing a method of claim 14, wherein storing a plurality of user-specific versions comprises storing a user-specific version in a user account for each of a plurality of users.

**Claim 16: See Sutter on col.89, lines 53-54;** discussing a method of claim 14, wherein obtaining an encryption component comprises obtaining an application security encryption key.

**Claim 17: See Sutter on col.89, lines 43-446 and 53-57;** discussing a method of claim 14, wherein creating a plurality of user-specific versions comprises encrypting the encryption component based on a plurality of different user passwords.

**Claim 18: See Sutter on col.90, lines 11-31;** discussing a method of claim 14, wherein selectively allowing users to process their version of the encryption component comprises authenticating users and only allowing authorized users to process their version of the encryption component.

**Claim 19: See Sutter on col.89, lines 43-446 and 53-57 and col.90, lines 11-31;** discussing a method of claim 18, wherein authenticating users comprises, for each user: receiving a password; processing the password to generate an encrypted version; and comparing the encrypted version to an authorized value.

**Claim 20: See Sutter on col.48, line 60 – col.49, line 65;** discussing a method of claim 19, wherein processing the password comprising applying a one-way hash algorithm.

**Claim 21: See Sutter on col.89, lines 43-446 and 53-57 and col.90, lines 11-31;;** discussing a computer implemented method of providing data security, the method comprising: receiving a password from a user; processing the password to form an encrypted version; comparing the encrypted version to a list of authorized values stored in a database; if the encrypted version matches an authorized value, and if doing so would be consistent with a plurality of allocated user access privileges, utilizing the password as a basis for decrypting a user-specific version of an encryption component; and utilizing the encryption component to process sensitive data.

Art Unit: 2135

**Claim 22: See Sutter on col.14, lines 2-6 and col.85, lines 25-36;**

discussing a method of claim 21, wherein the plurality of allocated user access privileges are distributed based on a plurality of user roles, and wherein the method further comprises making the step of utilizing the encryption component contingent upon the user being associated with a particular user role.

**Claim 23: See Sutter on col.14, lines 2-6 and col.85, lines 25-65;**

discussing a method of claim 21, wherein the plurality of allocated user access privileges are distributed based on user identity, and wherein the method further comprises making the steps of utilizing the encryption component contingent upon the user having a particular identity.

### ***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2135

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

LHa

  
AU2135